

SEQUENCES OF IRREDUCIBLE POLYNOMIALS OVER ODD PRIME FIELDS VIA ELLIPTIC CURVE ENDOMORPHISMS, II

S. UGOLINI

ABSTRACT. In this paper we extend a previous investigation by us regarding an iterative construction of irreducible polynomials over finite fields of odd characteristic. In particular, we show how it is possible to iteratively construct irreducible polynomials by means of two families of transforms, which we call the Q_k and \hat{Q}_k -transforms, related to certain degree two isogenies over elliptic curves, which split the multiplication-by-2 map.

1. INTRODUCTION

Inspired by the Q -transform and the R -transform (see [1], [2]), in [4] we defined the Q_k -transforms over any finite field of odd characteristic as follows.

If p is an odd prime, q is a power of p and $k \in \mathbf{F}_p^*$, then the Q_k -transform takes any polynomial $f \in \mathbf{F}_p[x]$ of positive degree n to

$$f^{Q_k}(x) = \left(\frac{x}{k}\right)^n \cdot f(\vartheta_k(x)),$$

where ϑ_k is the map which takes any element $x \in \mathbf{P}^1(\mathbf{F}_q) = \mathbf{F}_q \cup \{\infty\}$ to

$$\vartheta_k(x) = \begin{cases} \infty & \text{if } x = 0 \text{ or } \infty, \\ k \cdot (x + x^{-1}) & \text{otherwise.} \end{cases}$$

In [4] we showed how one can construct sequences of irreducible polynomials over finite fields by repeated applications of the Q_k -transforms when k and p fall into one of the following cases:

- $k \equiv \pm \frac{1}{2} \pmod{p}$;
- k is a root of $x^2 + \frac{1}{4}$ and $p \equiv 1 \pmod{4}$;
- k or $-k$ is a root of $x^2 + \frac{1}{2}x + \frac{1}{2}$ and $p \equiv 1, 2, \text{ or } 4 \pmod{7}$.

Since the dynamics of the maps ϑ_k seems to be chaotic for any k different from the aforementioned values, in this paper we illustrate an iterative construction of irreducible polynomials, which is independent of the characteristic of the field and employs two families of transforms, namely the Q_k -transforms and the \hat{Q}_k -transforms, which are below introduced.

We notice that if k is a quadratic residue in \mathbf{F}_p^* and α_k is a square root of k^3 in \mathbf{F}_p^* , then the map ϑ_k is involved in the definition of the isogeny

$$\psi_k(x, y) = \left(\vartheta_k(x), \alpha_k \cdot \frac{x^2 y - y}{x^2} \right)$$

from the elliptic curve

$$E : y^2 = x^3 + x$$

to the elliptic curve

$$E_k : y^2 = x^3 - 4k^2x.$$

Consider now the map $\hat{\vartheta}_k$ which takes any element $x \in \mathbf{P}^1(\mathbf{F}_q)$ to

$$\hat{\vartheta}_k(x) = \begin{cases} \infty & \text{if } x = 0 \text{ or } \infty, \\ \frac{x^2 - 4k^2}{4kx} & \text{otherwise,} \end{cases}$$

and the \hat{Q}_k -transform, which takes any polynomial $f \in \mathbf{F}_p[x]$ of positive degree n to

$$f^{\hat{Q}_k}(x) = (4kx)^n \cdot f(\hat{\vartheta}_k(x)).$$

The map $\hat{\vartheta}_k$ is involved in the definition of the isogeny

$$\hat{\psi}_k(x, y) = \left(\hat{\vartheta}_k(x), \frac{y(x^2 + 4k^2)}{8\alpha_k x^2} \right)$$

from E_k to E , namely the dual isogeny of ψ_k . If we denote by $[2]$ the duplication map on E , then

$$[2] = \hat{\psi}_k \circ \psi_k.$$

While the isogenies ψ_k and $\hat{\psi}_k$ have been defined only for the quadratic residues k in \mathbf{F}_p^* , the construction of sequences of irreducible polynomials, which is described in Section 3, can be carried over to any $k \in \mathbf{F}_p^*$, as explained in Remark 2.1.

2. PRELIMINARIES

Let \mathbf{F}_q be a finite field of odd characteristic p .

The structure of the group $E(\mathbf{F}_q)$ of rational points of E over \mathbf{F}_q depends upon p . In fact, if $p \equiv 1 \pmod{4}$, then E is an ordinary elliptic curve, while E is supersingular if $p \equiv 3 \pmod{4}$ (see [5, Proposition 4.37]).

Whichever p is, we can consider the map $[\tilde{2}]$ defined over $\mathbf{P}^1(\overline{\mathbf{F}}_q)$ as

$$[\tilde{2}] : x \mapsto \begin{cases} \infty & \text{if } x \in \{0, i_p, -i_p, \infty\}, \\ \frac{x^4 - 2x^2 + 1}{4(x^3 + x)} & \text{otherwise,} \end{cases}$$

where i_p is a square root of -1 in $\overline{\mathbf{F}}_p$.

For any $x \in \mathbf{P}^1(\overline{\mathbf{F}}_q)$ and any quadratic residue $k \in \mathbf{F}_p^*$ we have that

$$[\tilde{2}](x) = \hat{\vartheta}_k(\vartheta_k(x)). \quad (2.1)$$

Remark 2.1. While in the current section k is assumed to be a quadratic residue in \mathbf{F}_p^* , we notice that $[\tilde{2}] = \hat{\vartheta}_k \circ \vartheta_k$ whichever $k \in \mathbf{F}_p^*$ we take. This fact will let us to extend our iterative construction of irreducible polynomials in Section 3 to any k .

We can construct the functional graph $G_{[\tilde{2}]}^q$ of $[\tilde{2}]$ over $\mathbf{P}^1(\mathbf{F}_q)$, where the vertices are the elements of $\mathbf{P}^1(\mathbf{F}_q)$ and an arrow joins a vertex α to a vertex β if $\beta = [\tilde{2}](\alpha)$. Since any vertex of $G_{[\tilde{2}]}^q$ is either $[\tilde{2}]$ -periodic or preperiodic, any connected component of $G_{[\tilde{2}]}^q$ contains exactly one cycle, whose vertices are roots of reversed trees. In the following, for any non-negative integer i and any $[\tilde{2}]$ -periodic element $x_0 \in \mathbf{P}^1(\mathbf{F}_q)$, we denote by $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ the reversed tree of $G_{[\tilde{2}]}^{q^{2^i}}$ rooted in x_0 .

The following holds.

Lemma 2.2. *If $\tilde{x} \in \mathbf{P}^1(\overline{\mathbf{F}}_q)$, then*

$$|\{x \in \mathbf{P}^1(\overline{\mathbf{F}}_q) : [\tilde{2}](x) = \tilde{x}\}| = \begin{cases} 2 & \text{if } \tilde{x} \in \{\pm i_p, 0\}, \\ 4 & \text{otherwise.} \end{cases}$$

Proof. We introduce the following notations for any $x_0 \in \mathbf{P}^1(\overline{\mathbf{F}}_q)$:

$$\begin{aligned} \vartheta_k^{-1}\{x_0\} &= \{x \in \mathbf{P}^1(\overline{\mathbf{F}}_q) : \vartheta_k(x) = x_0\}; \\ \hat{\vartheta}_k^{-1}\{x_0\} &= \{x \in \mathbf{P}^1(\overline{\mathbf{F}}_q) : \hat{\vartheta}_k(x) = x_0\}; \\ [\tilde{2}]^{-1}\{x_0\} &= \{x \in \mathbf{P}^1(\overline{\mathbf{F}}_q) : [\tilde{2}](x) = x_0\}. \end{aligned}$$

We have that

$$\begin{aligned} |\vartheta_k^{-1}\{x_0\}| &= \begin{cases} 1 & \text{if } x_0 \in \{\pm 2k\}, \\ 2 & \text{otherwise,} \end{cases} \\ |\hat{\vartheta}_k^{-1}\{x_0\}| &= \begin{cases} 1 & \text{if } x_0 \in \{\pm i_p\}, \\ 2 & \text{otherwise.} \end{cases} \end{aligned}$$

Moreover,

$$\begin{aligned} \hat{\vartheta}_k\{\pm 2ki_p\} &= \{\pm i_p\}, \\ \hat{\vartheta}_k\{\pm 2k\} &= \{0\}. \end{aligned}$$

We can now analyse the different cases.

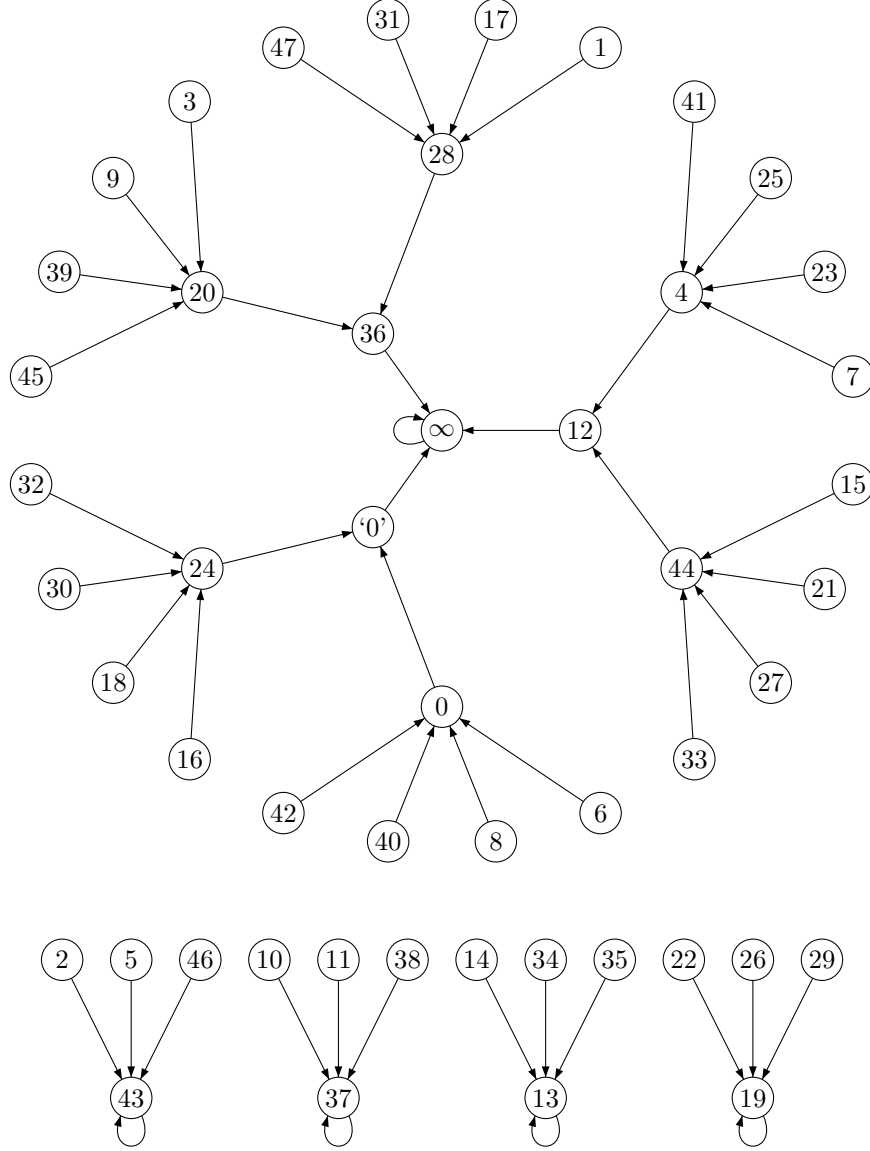
- If $\tilde{x} \in \mathbf{P}^1(\mathbf{F}_q) \setminus \{\pm i_p, 0\}$, then $\hat{\vartheta}_k^{-1}\{\tilde{x}\} = \{x_1, x_2\}$, where $\{x_1, x_2\} \cap \{\pm 2k\} = \emptyset$. Therefore, $|\left[\tilde{2}\right]^{-1}\{\tilde{x}\}| = 4$.
- If $\tilde{x} \in \{\pm i_p\}$, then $\hat{\vartheta}_k^{-1}\{\tilde{x}\} = \{2k\tilde{x}\}$. Therefore, $|\left[\tilde{2}\right]^{-1}\{\tilde{x}\}| = 2$.
- If $\tilde{x} = 0$, then $\hat{\vartheta}_k^{-1}\{\tilde{x}\} = \{\pm 2k\}$. Therefore, $|\left[\tilde{2}\right]^{-1}\{\tilde{x}\}| = 2$.

All considered, the result follows. \square

According to Lemma 2.2 the following holds.

Corollary 2.3. *Let $x_0 \in \mathbf{P}^1(\mathbf{F}_q)$ be $[\tilde{2}]$ -periodic. Then, $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ is a 4-ary tree for any non-negative integer i .*

Example 2.4. Below is represented the graph $G_{[\tilde{2}]}^{49}$. As regards the labels of the nodes, ‘0’ is the zero in \mathbf{F}_{49} , while all the other labels different from ∞ refer to the exponents of the powers α^i , being α a generator of the field \mathbf{F}_{49} . We notice that every node, which is not a leaf, has exactly 4 children, except for 12, 36 and ‘0’. This fact is in accordance with Lemma 2.2, since $(\alpha^{12})^2 = (\alpha^{36})^2 = -1$.



2.1. The ordinary case. In [3, Section 3] and in [4, Section 2.1], relying upon [6], we studied some properties of the group of rational points of E over a finite field. We summarize the relevant facts for the reader's convenience.

Let m be a positive integer, l a non-negative integer and $q = p^{2^l m}$. If we set $R = \mathbf{Z}[i]$ and denote by π_p the representation in R of the Frobenius endomorphism of E , then

$$E(\mathbf{F}_{p^{2^l m}}) \cong R/(\pi_p^{2^l m} - 1)R \cong R/\rho_0^{e_l} R \times R/\rho_1 R,$$

where $\rho_0 = 1 + i$, e_l is a non-negative integer which depends on l and ρ_1 is an element of R coprime to ρ_0 such that $\rho_0^{e_l} \cdot \rho_1 = \pi_p^{2^l m} - 1$. According to [4, Lemma 2.13 (1), (4)], the following holds.

Lemma 2.5. *We have that*

- $e_l \geq 2$;
- $e_l = e_{l-1} + 2$, if $l \geq 2$.

Since $[2] = \hat{\psi}_k \circ \psi_k$ and $2 = -i \cdot \rho_0^2$ in R , we can prove the forthcoming result concerning the depth of the trees rooted in $[\tilde{2}]$ -periodic elements of $G_{[\tilde{2}]}^q$.

Theorem 2.6. *Let $x_0 \in \mathbf{P}^1(\mathbf{F}_q)$ be $[\tilde{2}]$ -periodic. Then,*

- (1) $T_{[\tilde{2}]}^{q^2}(x_0)$ has depth $d := \lceil \frac{e_l+1}{2} \rceil$ and its leaves have height at least $d-1$;
- (2) the children of the leaves of $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ in $\mathbf{P}^1(\overline{\mathbf{F}}_q)$ are leaves of $T_{[\tilde{2}]}^{q^{2^{i+1}}}(x_0)$, for any positive integer i .

Proof. (1) The dynamics of $[\tilde{2}]$ over $\mathbf{P}^1(\mathbf{F}_{q^2})$ can be studied relying upon the iterations of $[2] = [-i\rho_0^2]$ in

$$R/(\pi_p^{2^{l+1}m} - 1)R \cong S = R/\rho_0^{e_l+1}R \times R/\rho_1R.$$

By hypothesis, $x_0 \in \mathbf{P}^1(\mathbf{F}_q)$. Therefore, either $x_0 = \infty$ or $(x_0, y_0) \in E(\mathbf{F}_{q^2})$, for some $y_0 \in \mathbf{F}_{q^2}$. In both cases, the corresponding point Q in S is of the form $Q = (0, Q_1)$.

Consider the point $P = ([1], [2]^{-d}Q_1) \in S$. Then, $[2]^d P = Q$, while $[2]^h P \neq Q$ for any positive integer $h < d$. More in general, if $(P_0, P_1) \in S$, then $[2]^d P_0 = 0$ in $R/\rho_0^{e_l+1}R$. Hence, $T_{[\tilde{2}]}^{q^2}(x_0)$ has depth d .

Let now \tilde{x} be a leaf of $T_{[\tilde{2}]}^{q^2}(x_0)$. Suppose that $P = (P_0, P_1)$ is the point in S having such a x -coordinate and that $P_0 = [a]$ for some $a \in R$. Then, $\rho_0^2 \nmid a$. Indeed, if $a = \rho_0^2 c$ for some $c \in R$, then we could take the point $\tilde{P} = ([ic], [2]^{-1}P_1)$ and notice that $[2]\tilde{P} = P$, which is absurd, since \tilde{x} is a leaf of the tree. Consequently, if $[2]^h P_0 = 0$ for some positive integer h , then $h \geq \lceil \frac{e_l+1}{2} \rceil - 1$.

- (2) Consider a leaf \tilde{x} of $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$, for some positive integer i . Let x' be one of the direct predecessors of \tilde{x} in $T_{[\tilde{2}]}^{q^{2^{i+1}}}(x_0)$. Since the greatest power of ρ_0 which divides $\pi_p^{2^{l+i+1}m} - 1$ is e_{l+i+1} and $e_{l+i+1} = e_{l+i} + 2$ according to Lemma 2.5, we have that x' is a leaf of $T_{[\tilde{2}]}^{q^{2^{i+1}}}(x_0)$. □

2.2. The supersingular case. Let i and m be two positive integers. Then, according to [6, Theorem 4.1],

$$E(\mathbf{F}_{p^{2^i m}}) \cong \mathbf{Z}/((-p)^{2^{i-1}m} - 1)\mathbf{Z} \times \mathbf{Z}/((-p)^{2^{i-1}m} - 1)\mathbf{Z}.$$

The following holds.

Lemma 2.7. *There exist two positive integers e_{i-1} and e_i and two odd integers r and s such that*

$$\begin{aligned} (-p)^{2^{i-1}m} - 1 &= 2^{e_{i-1}} \cdot r, \\ (-p)^{2^i m} - 1 &= 2^{e_i} \cdot s. \end{aligned}$$

Moreover, $e_i = e_{i-1} + 1$.

Proof. Since $-p \equiv 1 \pmod{4}$, we have that

$$\begin{aligned} (-p)^{2^{i-1}m} - 1 &\equiv 0 \pmod{4}, \\ (-p)^{2^{i-1}m} + 1 &\equiv 2 \pmod{4}. \end{aligned}$$

Therefore,

$$\begin{aligned} (-p)^{2^{i-1}m} - 1 &= 2^{e_{i-1}} \cdot r, \\ (-p)^{2^{i-1}m} + 1 &= 2 \cdot r', \end{aligned}$$

for some integer $e_{i-1} \geq 2$ and some odd integers r and r' . Hence,

$$(-p)^{2^i m} - 1 = ((-p)^{2^{i-1}m} - 1) \cdot ((-p)^{2^{i-1}m} + 1) = 2^{e_{i-1}+1} \cdot r \cdot r'.$$

The result follows setting $e_i = e_{i-1} + 1$ and $s = r \cdot r'$. \square

According to Lemma 2.7, if we set $q = p^m$, then

$$E(\mathbf{F}_{q^{2^i}}) \cong S_i = (\mathbf{Z}/2^{e_{i-1}}\mathbf{Z} \times \mathbf{Z}/r\mathbf{Z})^2.$$

The following holds.

Theorem 2.8. *Let $x_0 \in \mathbf{P}^1(\mathbf{F}_q)$ be $[\tilde{2}]$ -periodic. Then*

- (1) $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ has depth e_{i-1} ;
- (2) the children of the leaves of $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ in $\mathbf{P}^1(\overline{\mathbf{F}}_q)$ are leaves of $T_{[\tilde{2}]}^{q^{2^{i+1}}}(x_0)$.

Proof. (1) Since x_0 is $[\tilde{2}]$ -periodic in $\mathbf{P}^1(\mathbf{F}_q)$, it is the x -coordinate of a rational point in $E(\mathbf{F}_{q^{2^i}})$, which corresponds to a point in S_i of the form

$$([0], [a_r], [0], [b_r])$$

for some integers a_r and b_r . We notice that e_{i-1} is the smallest positive integer k such that $[2]^k[c] = [0]$ for any $[c]$ in $\mathbf{Z}/2^{e_{i-1}}\mathbf{Z}$. Indeed, any leaf of $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ is the x -coordinate of a point

$$([a_2], [2]^{-e_{i-1}}[a_r], [b_2], [2]^{-e_{i-1}}[b_r])$$

in S_i for some integers a_2 and b_2 which are not both divisible by 2 in \mathbf{Z} . Therefore, the tree $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ has depth e_{i-1} and, in analogy, $T_{[\tilde{2}]}^{q^{2^{i+1}}}(x_0)$ has depth e_i .

- (2) Any leaf of $T_{[\tilde{2}]}^{q^{2^i}}(x_0)$ lies on the level e_{i-1} of the tree $T_{[\tilde{2}]}^{q^{2^{i+1}}}(x_0)$, which has depth e_i . Consequently, its children are leaves of $T_{[\tilde{2}]}^{q^{2^{i+1}}}(x_0)$. \square

Example 2.9. Let $q = 7^2$. Then,

$$E(\mathbf{F}_{7^2}) \cong \mathbf{Z}/(-8)\mathbf{Z} \times \mathbf{Z}/(-8)\mathbf{Z}.$$

According to Theorem 2.8, any $[\tilde{2}]$ -periodic element $x_0 \in \mathbf{P}^1(\mathbf{F}_{49})$ is root of a tree having depth 3. This is the case of ∞ , as we can see in Example 2.4.

3. CONSTRUCTING SEQUENCES OF IRREDUCIBLE POLYNOMIALS

Let f be a monic irreducible polynomial of positive degree n belonging to $\mathbf{F}_p[x]$, for some odd prime p , and set $q = p^n$. For a fixed $k \in \mathbf{F}_p^*$ we can construct two sequences $\{g_i\}_{i \geq 0}$ and $\{h_i\}_{i \geq 0}$ of monic irreducible polynomials as follows.

- We set $g_0 := f$ and $h_0 := f$.
- We set $g_1 := f^{\hat{Q}_k}$ and $h_1 := f^{\hat{Q}_k}$, if $f^{\hat{Q}_k}$ is irreducible. Otherwise, we set g_1 equal to one of the two monic irreducible factors of $f^{\hat{Q}_k}$ and h_1 equal to the other factor.
- For any positive integer i we set g_i (resp. h_i) equal to
 - one of the monic irreducible factors of $g_{i-1}^{\hat{Q}_k}$ (resp. $h_{i-1}^{\hat{Q}_k}$), if i is odd;
 - one of the monic irreducible factors of $g_{i-1}^{Q_k}$ (resp. $h_{i-1}^{Q_k}$), if i is even.

Remark 3.1. We notice in passing that if $\tilde{f} \in \mathbf{F}_p[x]$ is irreducible of degree m , then either \tilde{f}^{Q_k} (resp. $\tilde{f}^{\hat{Q}_k}$) is irreducible of degree $2m$, or it splits into the product of two irreducible factors of degree m . Indeed, if α is a root of \tilde{f}^{Q_k} (resp. $\tilde{f}^{\hat{Q}_k}$), then $f(\vartheta_k(\alpha)) = 0$ (resp. $f(\hat{\vartheta}_k(\alpha)) = 0$). Hence, either α has degree $2m$ or it has degree m over \mathbf{F}_p .

The following holds.

Lemma 3.2. *If \tilde{x} is a root of f in \mathbf{F}_q , then*

- (1) *\tilde{x} belongs to the level r of the tree $T_{[2]}^q(x_0)$, for some non-negative integer r and $x_0 \in \mathbf{P}^1(\mathbf{F}_q)$;*
- (2) *for any positive integer j , either any polynomial g_{2j} or any polynomial h_{2j} has a root \tilde{x}_j belonging to the level $r + j$ of the tree $T_{[2]}^{q^{2^i}}(x_0)$ for some non-negative integer i .*

Proof. We prove separately the two assertions.

- (1) The assertion holds because any element in $\mathbf{P}^1(\mathbf{F}_q)$ is either $[\tilde{2}]$ -periodic or preperiodic. In the former case $x_0 = \tilde{x}$, while in the latter case some iterate of \tilde{x} is $[\tilde{2}]$ -periodic and we set x_0 equal to the first of such iterates which is $[\tilde{2}]$ -periodic.
- (2) The assertion can be proved by induction on j .

First we define $\tilde{g} := g_0^{\hat{Q}_k}$. We notice that g_2 and h_2 are factors of \tilde{g}^{Q_k} . Since $[\tilde{2}] = \hat{\vartheta}_k \circ \vartheta_k$, the (at most) 4 preimages of \tilde{x} with respect to the map $[\tilde{2}]$ in $\mathbf{P}^1(\mathbf{F}_q)$ are roots of \tilde{g}^{Q_k} . Moreover, at most one of the preimages is $[\tilde{2}]$ -periodic. Therefore, without loss of generality, we can suppose that g_2 has a root which is not $[\tilde{2}]$ -periodic. If we denote by \tilde{x}_1 such a root, then the base step is proved.

As regards the inductive step, suppose that g_{2j} has a root \tilde{x}_j belonging to the level $r + j$ of the tree $T_{[2]}^{q^{2^i}}(x_0)$ for some positive integers i and j . Using the same argument as above, we can define $\tilde{g} := g_{2j}^{\hat{Q}_k}$ and notice that g_{2j+2} is a factor of \tilde{g}^{Q_k} . Therefore, the preimages of \tilde{x}_j in $T_{[2]}^{q^{2^{i+1}}}(x_0)$ are roots of \tilde{g}^{Q_k} . One of the preimages, which we denote by \tilde{x}_{j+1} , is a root of g_{2j+2} and the inductive step is proved. □

We discuss the ordinary and the supersingular case separately.

3.1. Ordinary case: $p \equiv 1 \pmod{4}$. Suppose that $\pi_p^{2n} - 1 = \rho_0^{e_1} \cdot \rho_1$, for some positive integer e_1 and some element $\rho_1 \in R$ coprime to ρ_0 . The following holds.

Theorem 3.3. *There exists a positive integer $t \leq \left\lceil \frac{e_1}{2} \right\rceil$ such that at least one of the following holds:*

- g_{t+2j-1} and g_{t+2j} have degree $2^{1+j} \cdot n$ for any integer $j \geq 1$;
- h_{t+2j-1} and h_{t+2j} have degree $2^{1+j} \cdot n$ for any integer $j \geq 1$.

Proof. Adopting the notations of Section 2.1, let $m = n$, $q = p^m$ and $l = 0$. In accordance with Lemma 3.2(2), we can say without loss of generality that, for any positive integer j , any polynomial g_{2j} has a root belonging to the level $r + j$ of the tree $T_{[2]}^{q^{2^i}}(x_0)$, for some $x_0 \in \mathbf{P}^1(\mathbf{F}_q)$ and for some non-negative integer i . According to Theorem 2.6(1), the tree $T_{[2]}^{q^2}(x_0)$ has depth $\left\lceil \frac{e_1}{2} \right\rceil$. Let t be the smallest index $2j$ such that g_{2j} has a root in \mathbf{F}_{q^2} , while g_{2j+2} has a root in $\mathbf{F}_{q^{2^2}}$. The result follows because the degree of g_{t+2j} is twice the degree of $g_{t+2(j-1)}$ for any integer $j \geq 1$ and the result follows according to Theorem 2.6(2). \square

3.2. Supersingular case: $p \equiv 3 \pmod{4}$. Suppose that $p \equiv 3 \pmod{4}$ and that $(-p)^n - 1 = 2^{e_0} \cdot r$, for some integers e_0 and r . The following holds.

Theorem 3.4. *There exists a positive integer $t \leq e_0$ such that at least one of the following holds:*

- g_{t+2j-1} and g_{t+2j} have degree $2^{1+j} \cdot n$ for any integer $j \geq 1$;
- h_{t+2j-1} and h_{t+2j} have degree $2^{1+j} \cdot n$ for any integer $j \geq 1$.

Proof. The current theorem can be proved as Theorem 3.3 relying upon Theorem 2.8 and Lemma 3.2. \square

REFERENCES

1. S. D. Cohen, *The explicit construction of irreducible polynomials over finite fields*, Des. Codes Cryptogr. **2** (1992), no. 2, 169–174.
2. H. Meyn, *On the construction of irreducible self-reciprocal polynomials over finite fields*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), no. 1, 43–53.
3. S. Ugolini, *On the iterations of certain maps $X \mapsto K \cdot (X + X^{-1})$ over finite fields of odd characteristic*, J. Number Theory **142** (2014), 274–297.
4. ———, *Sequences of irreducible polynomials over odd prime fields via elliptic curve endomorphisms*, J. Number Theory **152** (2015), 21–37.
5. L. C. Washington, *Elliptic curves: number theory and cryptography*, CRC Press, Boca Raton, 2008.
6. C. Wittmann, *Group structure of elliptic curves over finite fields*, J. Number Theory **88** (2001), 335–344.

E-mail address: sugolini@gmail.com